INSTITUTE OF DIRECTORS
IN IRELAND

Director Sentiment Monitor

Quarterly Members' Survey
Q4 2022

February 2023

www.iodireland.ie

The Institute of Directors in Ireland

The Institute of Directors (IoD) in Ireland is the leading membership body for directors and business leaders. Our purpose is to instill stakeholder trust and confidence in organisations by educating, informing, and supporting directors and business leaders to lead successfully. Our vision is for Ireland to be an exemplar of corporate governance.

Contents

Foreword

The world of cyber security is evolving constantly from increasing legislation to a changing threat landscape. The objective of this Director Sentiment Monitor was to understand the challenges and opportunities facing organisations with regard to cyber security. This research looks at the important role organisational leadership and governance has in combating cyber security threats.

In this Director Sentiment Monitor for Q4 2022, 41% of respondents told us their primary organisation has experienced a cyber attack. Interestingly, 36% of respondents said their primary organisation has cyber security as a standing item at all board meetings, while 27% said it was discussed quarterly. Among other findings, it is also encouraging that 81% of respondents said their primary organisation has a cyber security response plan in place.

Not so encouraging, however, is the finding that only 44% of respondents said their primary organisation has a cyber security training plan in place for board members, trailing considerably behind it having such a plan in place for senior executive management and for wider staff. It is crucial that board directors follow their duties as a director by carrying out their functions with care, skill, and diligence, including that of cyber security. Training is essential for an informed understanding of cyber security issues, plans, threats and responses.

Our latest research also finds that 70% of respondents are either extremely or very concerned about cyber security threats to the business continuity of their primary organisation.

Thank you to all IoD members who were able to take the time to respond to the survey.

Caroline Spillane CDir
Chief Executive Officer
Institute of Directors (IoD) in Ireland

Governance: Cyber Security

The governance of cyber security by boards of directors and senior management must evolve in line with the sophistication of the threat landscape, and the introduction of legislation and regulation towards protecting organisations and society from this threat. IoD Ireland has conducted this research to understand the challenges and opportunities facing organisations, and the actions members and their boards can take to build a resilient organisation and drive secure growth.

Effectively integrating the governance of cyber security into your company's overall governance framework is critical.

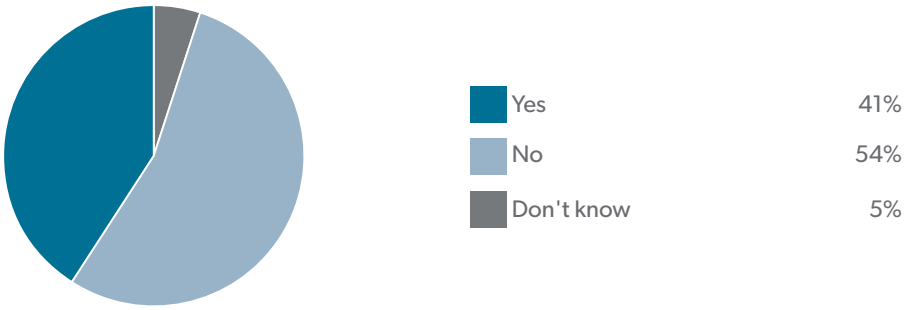
As with any form of organisational risk, the board of directors needs to identify, prioritise and develop mitigation strategies for its cyber risks, and inform cyber security resource allocation decisions. Key to board leadership in this area is a cyber security strategy, a cyber security incident response plan and effective and consistent cyber security training throughout the organisation. It is also key that cyber security features regularly on the agenda of board meetings to discuss risks and threats of cyber security attacks, receive updates on actual incidents of attacks and how they are being resolved, and to gain assurance on the systems of internal control. In this IoD member survey, our research touches on these areas, the objective being to enable members to critically reflect on the cyber security elements of their governance frameworks.

Incidents of Cyber Security Attacks

Our research tells us that 41% of respondents' organisations have experienced a cyber attack. Of those who responded 'yes', we then asked when this attack took place. 25% of respondents say the breach occurred in the last six months. Furthermore, 21% reveal it was in the last year, 32% say it was in the last two years, while 13% say it was in the last three years.

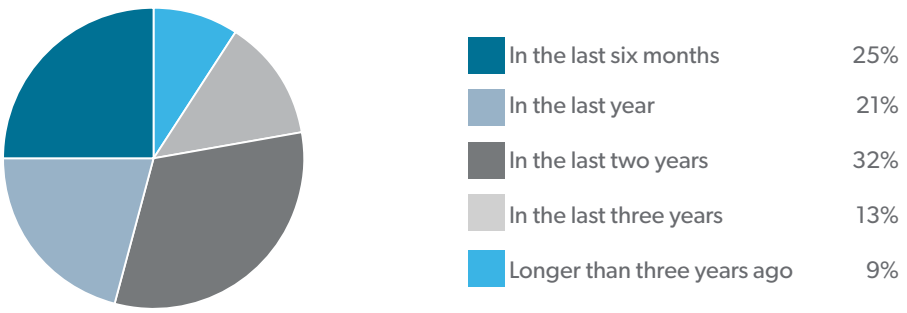
These findings highlight the present and significant risk of cyber security attacks to our respondent organisations. It is essential that all business leaders assess their own risk management and internal control frameworks to ensure that cyber risk is being effectively managed.

Figure 1: Has your primary organisation ever experienced a cyber security attack?



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

Figure 2: Did the attack happen…? (This question was asked of those who responded 'yes' in Figure 1.)



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

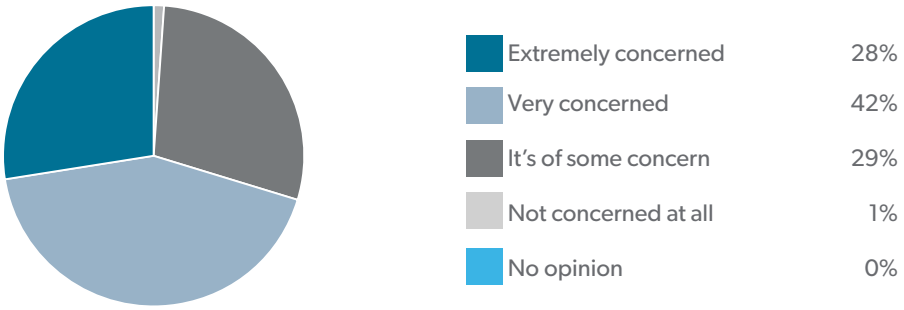
Governance: Cyber Security

Cyber Security Threats, Business Continuity and Operational Resilience

In these unpredictable and uncertain times, business continuity and operational resilience is an increasingly important area of governance in its own right. Our research finds that 70% of our respondents note that they are extremely or very concerned about the potential impact of cyber security threats to the business continuity of their primary organisation. Another 29% say it is of some concern. Just 1% of respondents are 'not concerned at all'.

The National Cyber Security Centre (NCSC) notes, 'operational resilience is about the ability of an organisation to recover from disruption, including those caused by cyber attacks. When the inevitable cyber attack does occur and damage and/or disruption is inflicted, an organisation's ability to recover quickly will be the key to its survival'.[1] It is highly recommended that an organisation's business continuity plan takes into consideration cyber security threats, and includes a plan of action. It may also be applicable for some organisations to establish a risk committee, which has been more common in financial services. However, as noted in the IoD Ireland Director Handbook, cyber risks have become an important consideration for most firms, not least financial services entities.[2]

Figure 3: How concerned are you about potential cyber security threats to the business continuity of your primary organisation?



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

[1] National Cyber Security Centre, '12 Steps to Cyber Security: Guidance on Cyber Security for Irish Business', *www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf*
[2] IoD Ireland, in partnership with McCannFitzGerald, Directors' Handbook (Fifth Edition), *www.iodireland.ie/resources-media/research-publications/director-handbooks/director-handbook*

Governance: Cyber Security

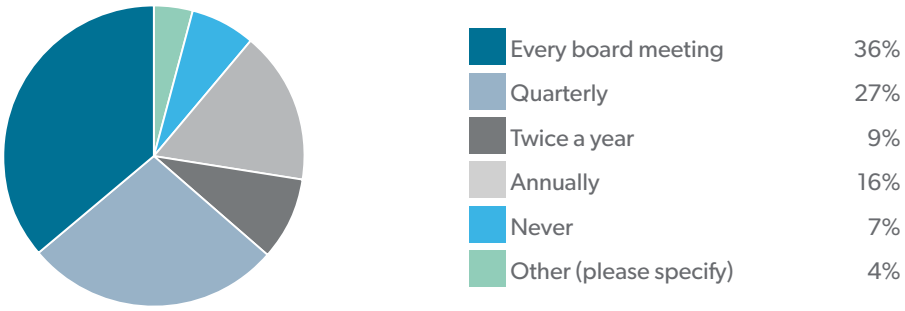
Cyber Security and Board Agendas

'Meeting frequently is one of the many ways to boost the priority given to cyber risk in business decisions,' according to the World Economic Forum's Global Security Outlook 2023 (WEF GCO 2023) report.[3]

With cyber security threats such a concern, it is no surprise that 36% of our respondents say that cyber security is on the agenda of every board meeting of their primary organisation. Furthermore, while 27% say it is on the agenda quarterly, 9% say twice yearly, and 16% say annually. It is encouraging to learn that 63% of respondents say cyber security is on their board agenda at least quarterly. The IoD would advocate that the frequency of discussion should correlate with the cyber risk appetite and exposure of the organisation. What is pivotal is that the board has agreed the basis of reporting provided to it by management (e.g. KPIs versus risk appetite, significant incident reports and efficacy of organisation response to such incidents, testing and related assurance on internal controls related to cyber security risks).

It is also imperative that board directors ask the right cyber security questions, and that the executive communicate this in an impactful way to ensure a full understanding of risks. The aforementioned WEF CGO 2023 report recommends that this is communicated reflecting the potential cyber risk to business continuity and the financial impact on a business. Furthermore, the WEF report notes that the return on investment of cyber security measures should also be clearly noted.[4]

Figure 4: In respect of your primary organisation how often is cyber security on the agenda of your board meeting?



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

[3] World Economic Forum, 'Global Cyber Security Outlook 2023', (January 2023), *www.weforum.org/reports/global-cybersecurity-outlook-2023/*
[4] Ibid

Governance: Cyber Security

Cyber Security Incidence Response Plan

It is encouraging that four out of five (81%) of respondents say their primary organisation has a cyber security incident response plan in place, while just 16% say it doesn't. This is a positive finding, and we would recommend that all organisations have a cyber security incident response plan in place.

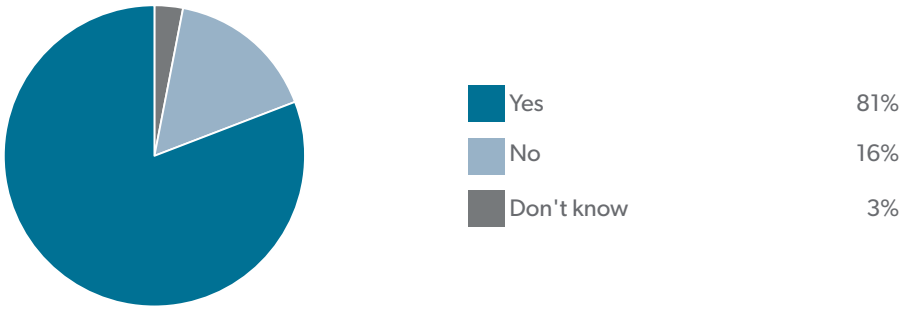
The National Cyber Security Centre (NCSC) recommends that organisations, 'establish an incident response and investigations capability including a formal team, who have been trained in and are following a documented plan, which is tested at least annually'.[5]

As outlined in the IoD Ireland Directors' Handbook, 'one of the General Duties of a Director under the Companies Act 2014 is that requirement of a director to perform his or her functions with care, skill and diligence'.[6]

It is important that directors continue to ask the right questions of the executive when hearing updates about cyber security incident response plans, such as: Is the plan tested? Does it take into consideration all stakeholders? Does it take into consideration all relevant law enforcement and regulated entities? How frequently does testing take place? What are the key learnings from tests completed?

The board should also challenge the design and roll-out of staff training on cyber security.

Figure 5: Does your primary organisation have a cyber security incident response plan in place?



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

[5] National Cyber Security Centre, '12 Steps to Cyber Security: Guidance on Cyber Security for Irish Business', *www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf*
[6] IoD Ireland, in partnership with McCannFitzGerald, Directors' Handbook (Fifth Edition), *www.iodireland.ie/resources-media/research-publications/director-handbooks/director-handbook*

Governance: Cyber Security

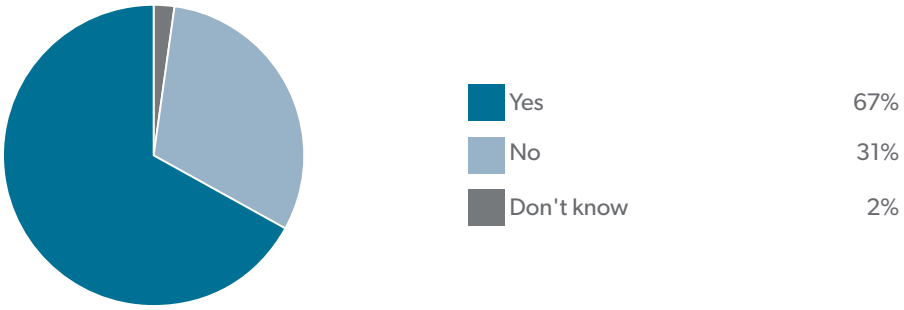
Cyber Security Strategy

The research found that 67% of respondents say their primary organisation has a board-approved IT and cyber security strategy, while nearly one-third of respondents say it doesn't. Indeed, it is essential that boards ensure that cyber security strategy is clearly articulated within their organisation and linked to the wider strategy and related risk appetite of the organisation.

The WEF GCO 2023 report found that 'incorporating cyber-resilience governance into their business strategy is one of the most impactful principles when it comes to cyber resilience'.[7]

It would be recommended for all boards to have a board approved IT and cyber security strategy in place.

Figure 6: Does your primary organisation have a board-approved IT and cyber security strategy?



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

[7] World Economic Forum, 'Global Cyber Security Outlook 2023', (January 2023), *www.weforum.org/reports/global-cybersecurity-outlook-2023/*

Governance: Cyber Security

Cyber Security Training

A cyber security training plan is a key pillar of any cyber security strategy. It is revealing that over half of respondents say their primary organisation does not have a cyber security plan in place for board members. This is despite 70% of respondents reporting they are extremely or very concerned about the potential impact of cyber security threats to the business continuity of their primary organisation.

Figure 7: Does your primary organisation have a cyber security training plan for board members, executive management and staff?

	Yes	No	Don't Know
Board Members	44%	51%	5%
Senior Executive Management	82%	14%	4%
Staff	79%	15%	6%

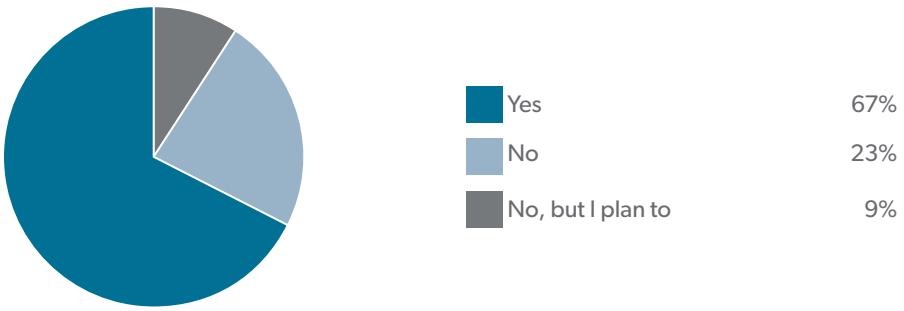
Source: IoD Ireland Director Sentiment Monitor Q4 2022.

In addition, when asked whether respondents had undertaken cyber security training in the last 12 months, 67% say they have. Furthermore, nearly a quarter (23%) say they have not, and 9 % say 'no, but I plan to' undertake such training.[8]

A cyber security incident can have a significantly negative impact on an organisation and can lead to reputational damage. As noted previously, it is essential that board directors are receiving the pertinent board information related to cyber security risk management and control. To interpret and challenge this effectively, it is crucial that directors continually refresh and update their expertise and training in cyber security.

According to Maya Bundt, Member of the World Economic Forum's Global Future Council on Cybersecurity: 'More and more corporate boards now have true cyber experts among their members. It helps when people at board level are sufficiently cyber-literate to ask pertinent questions of their security teams but also to bring cyber into strategic business discussions. Boards also need to understand what a cyber event means for their organization. Too many business leaders still underestimate the impact a cyberattack can have on their operations, on their reputation and on their company as a whole.'[9]

Figure 8: Have you undertaken cyber security training in the last 12 months?



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

[8] This question asked the respondents this as a whole, and it was not broken down to their role as a board director or a member of management.
[9] World Economic Forum, 'Global Cyber Security Outlook 2023', (January 2023), *www.weforum.org/reports/global-cybersecurity-outlook-2023/*

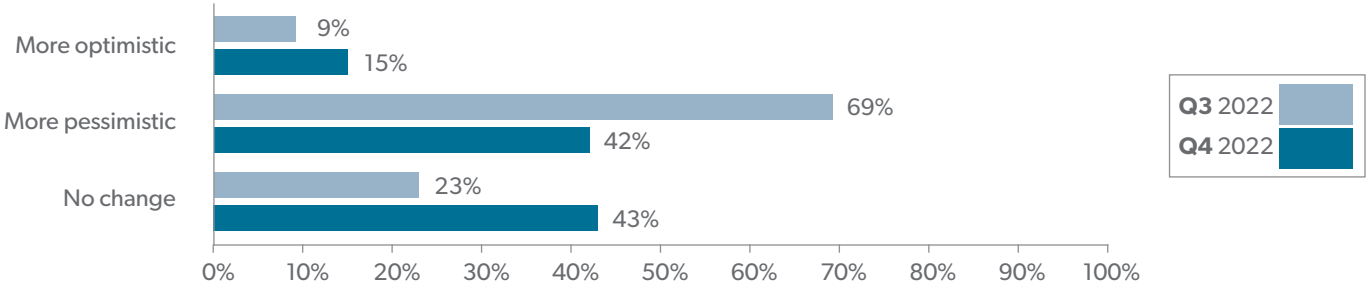
The Economy

Business Confidence and the Irish Economy

In our latest Q4 2022 research, 15% of business leaders are more optimistic about the Irish economy when compared to the previous quarter, Q3 2022, when it 9% of respondents were more optimistic. Year-on year, this finding has dropped 16% since Q4 2021, at that time 31% of business leaders were more optimistic.

It is no surprise, then, that 42% of business leaders are 'more pessimistic' about the economy in Q4 2022 compared to Q3 2022, when 69% were 'more pessimistic'. Year-on-year, this finding was 28% in Q4 2021.

Figure 9: Business confidence in the Irish economy in Q4 2022 compared to Q3 2022.



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

The Economy

Effect of Government's Performance

With regard to the effect of the Government's performance to date on consumer confidence, on the one hand, and business decision making, on the other hand, we are seeing largely more positive numbers in Q4 2022 than in Q3 2022.

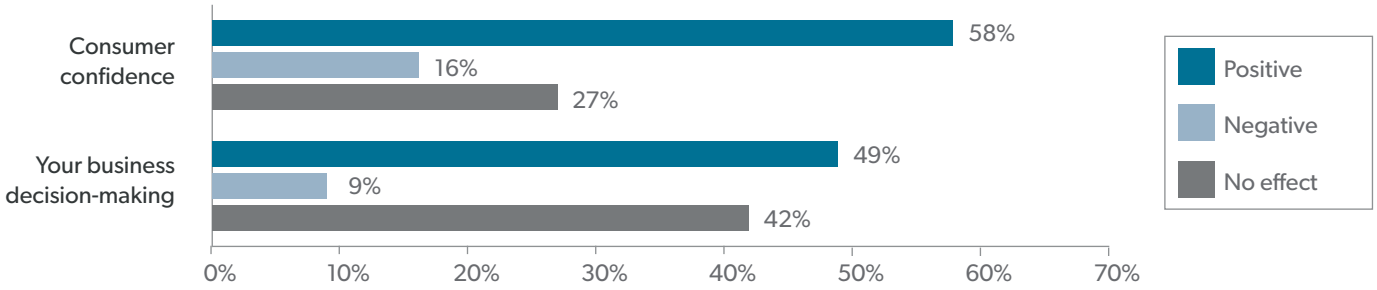
Consumer Confidence

- In Q4 2022, 58% of business leaders believed the effect of the current Government's performance on consumer confidence to be positive. This has increased from 34% in Q3 2022. Year-on-year, this figure was 36% in Q4 2021.
- In Q4 2022, 16% of business leaders believed the effect of the current Government's performance on consumer confidence to be negative. This has increased from 29% in Q3 2022. Year-on-year, this figure was 37% in Q4 2021.
- In Q4 2022, 27% of respondents say the Government's performance has had no effect on consumer confidence. This was 37% in Q3 2022. Year-on-year, this figure was 27% in Q4 2021.

Business Decision-Making

- In Q4 2022, 49% of business leaders believed the effect of the current Government's performance on their business decision making to be positive. This has increased from 31% in Q3 2022. Year-on-year, this figure was 32% in Q4 2021.
- In Q4 2022, 9% of business leaders believed the effect of the current Government's performance on their business decision making to be negative. This has decreased from 19% in Q3 2022. Year-on-year, this figure was 17% in Q4 2021.
- In Q4 2022, 42% of business leaders believed the Government's performance has had no effect on their business decision-making. This has decreased from 50% in Q3 2022. Year-on-year, this figure was 51% in Q4 2021.

Figure 10: What do you believe has been the effect of the current Government's performance to date on the following?



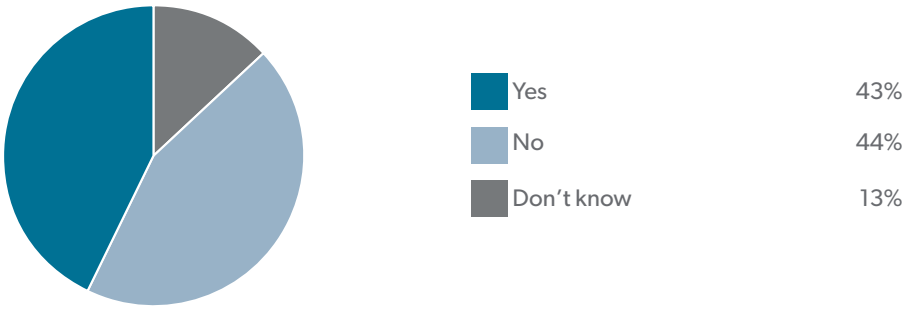
Source: IoD Ireland Director Sentiment Monitor Q4 2022.

Financial Performance

Financial Performance

- In our latest Q4 2022 research, 43% of our respondents believe the financial performance of their primary organisation will improve in Q1 2023, while 44% do not believe that will be the case.
- For a year-on-year comparison, in Q4 2021, nearly two-thirds (64%) of respondents believed the financial performance of their primary organisation would improve in Q1 2022 while 23% did not.

Figure 11: Do you think that the financial performance of your primary organisation will improve in Q1 2023?

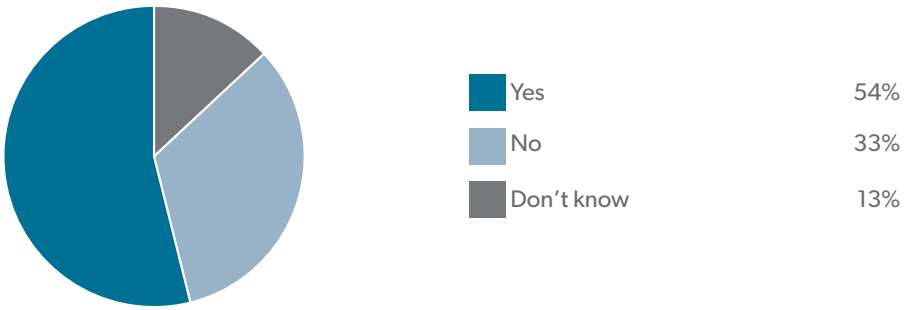


Source: IoD Ireland Director Sentiment Monitor Q4 2022.

In our latest research, 54% of respondents think the financial performance of their primary organisation will improve for the year 2023, while over one-third (33%) do not.

However, in a year-on-year comparison, when asked this question in Q4 2021, 77% of business leaders were hopeful the financial performance of their primary organisation would improve in 2022, while 14% were not.

Figure 12: Do you think that the financial performance of your primary organisation will improve for the year 2023?



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

Methodology

The Q4 2022 Director Sentiment Monitor had 307 respondents. In addition, 68% of the respondents are current board members, with the remainder in senior executive roles. The survey was issued to all IoD members, with a link to the online survey, and was carried out during the time period 25th of November to 14th December 2022.

For the purposes of comparison, data from previous IoD Ireland quarterly surveys is also included in this publication in certain instances. The findings in this research have been rounded up or down to the nearest decimal point. For the majority of questions, respondents were given the option of one response. In certain cases, these figures will not add up to 100% due to rounding up or down of percentages.

Research from the following publications has also been noted:

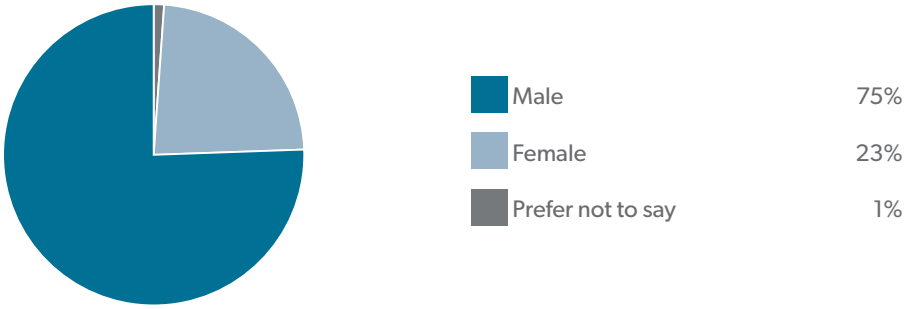
- IoD Ireland, in partnership with McCannFitzGerald, Directors' Handbook (Fifth Edition, 2023)
- World Economic Forum, 'Global Cybersecurity Outlook 2023' (January 2023)
- National Cyber Security Centre, '12 Steps on Cyber Security - Guidance on Cyber Security for Irish Business' (2018)

Demographics

Gender

In the Q4 2022 survey 75% of respondents were male and 23% were female.

Figure 13: Gender of respondents

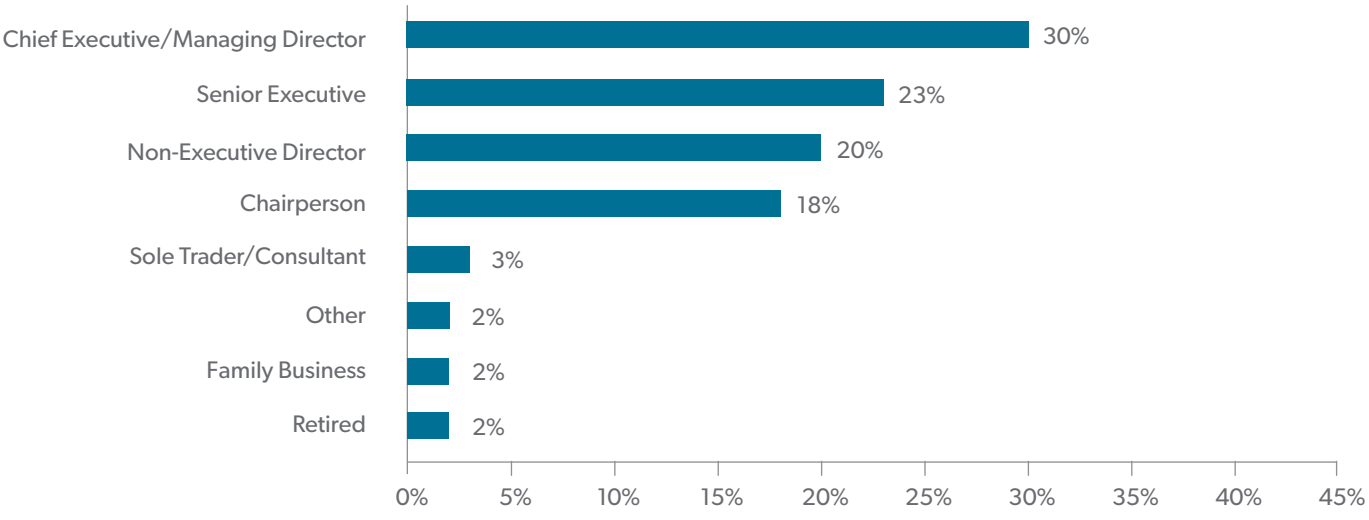


Source: IoD Ireland Director Sentiment Monitor Q4 2022.

Role/Position

The respondents to the Q4 2022 survey hold the following roles/positions:

Figure 14: Breakdown of respondents by role/position



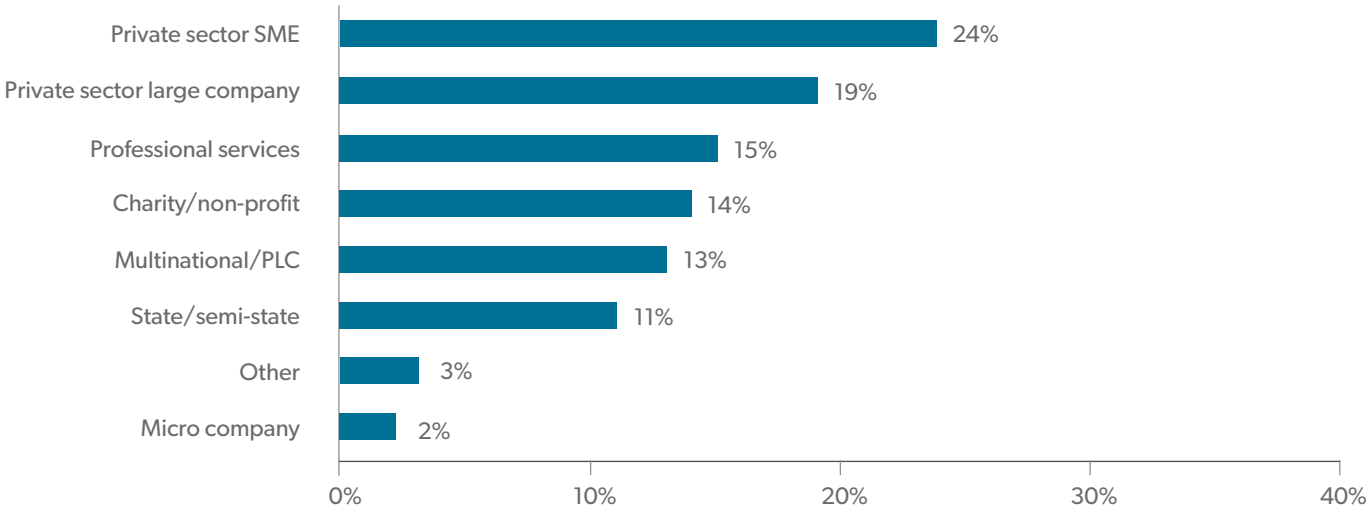
Source: IoD Ireland Director Sentiment Monitor Q4 2022.

Demographics

Company Type

The respondents to the Q4 2022 survey represent the following types of companies:

Figure 15: Breakdown of respondents by company type

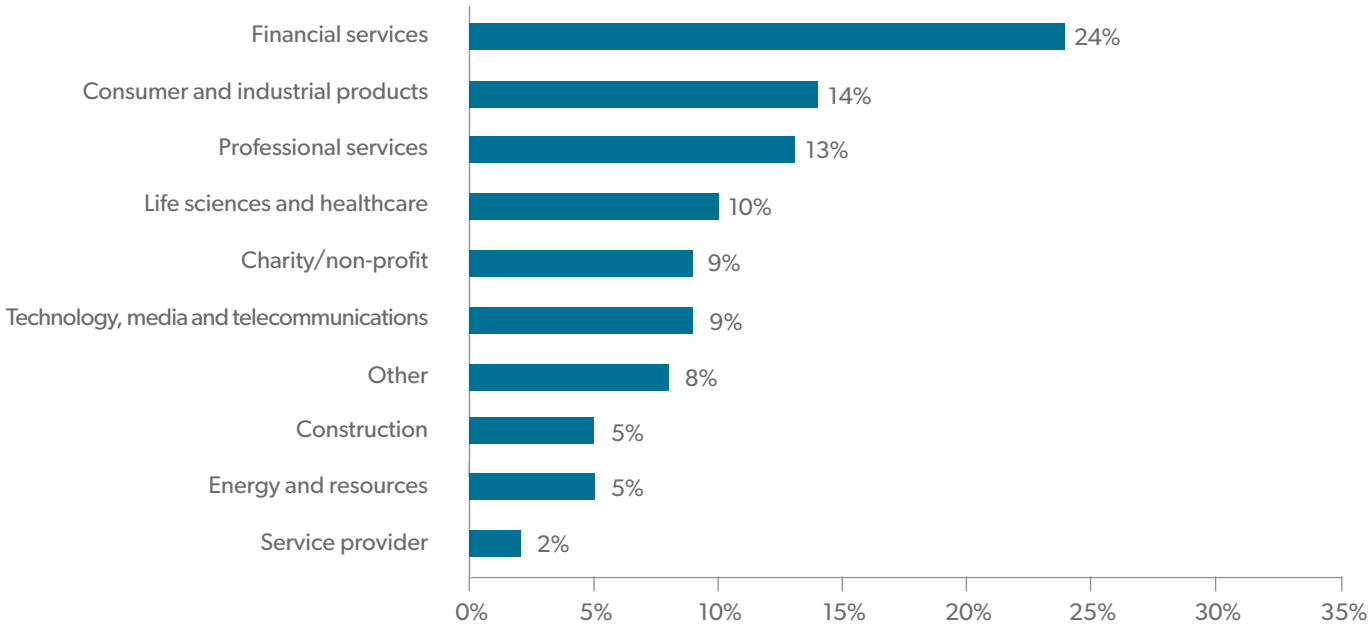


Source: IoD Ireland Director Sentiment Monitor Q4 2022.

Industry Sector

The respondents to the Q4 2022 survey operate in the following types of sectors:

Figure 16: Breakdown of respondents by industry sector

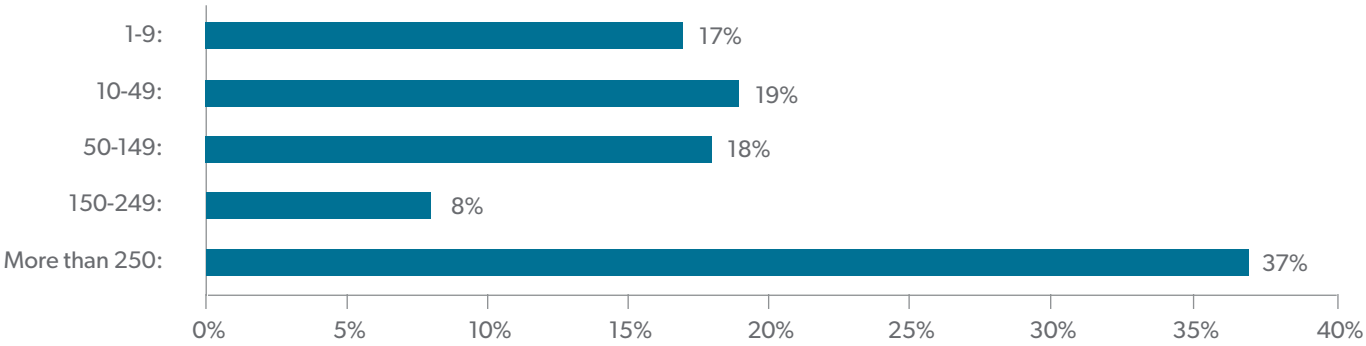


Source: IoD Ireland Director Sentiment Monitor Q4 2022.

Demographics

Employees

Figure 17: Employees by size category



Source: IoD Ireland Director Sentiment Monitor Q4 2022.

INSTITUTE OF DIRECTORS
IN IRELAND

Institute of Directors in Ireland

Tel: +353 1 411 0010
Email: comms@iodireland.ie
www.iodireland.ie